Acmetek

A Trusted Advisor of Security Solutions and Services

#TrustedPKIAdvisor

Install your SSL Certificate on Lync 2010

WHITE PAPER

https://www.acmetek.com

Microsoft Lync 2010 combines instant messaging, VoIP calling, live meetings, and videoconferencing, but it's more than the sum of these parts. Although Lync integrates with almost any PBX, it puts the PC at the center of communications so effectively that it could send your current phone system packing.

Lync provides clear VoIP calling and crisp videoconferencing without requiring special network accommodations. It integrates with Microsoft Exchange, Microsoft SharePoint, and Microsoft Office, bringing user presence information to Outlook and SharePoint team sites and allowing instant messages and phone calls to be initiated with a click.

Installation steps

1. On the Windows **Start** menu, click All **Programs** > **Microsoft Lync Server 2010** > **Lync Server Deployment Wizard**.
2. In the **Lync Server 2010 – Deployment Wizard**, click **Install or Update Lync Server System**.
3. Under **Step 3: Request, Install, or Assign Certificates**, click **Run**.
4. In the **Certificate Wizard**, select **External Edge certificate (public internet)** and then click **Import Certificate.**
5. On the **Import Certificate** page, enter or browse for the location of the certificate file.
   If you used the Lync interface to create the CSR, the certificate file is a .cer file (i.e. yourdo main_com.cer).
   If you used the DigiCert Certificate Utility to create the CSR, the certificate file is a .pfx file (i.e. yourdomain_com.pfx).
6. If you are using a .pfx file, check the **Certificate file that contains certificate's private key**.
   If you are using a .cer file, do not check this box.
7. Click **Next**.
8. On the **Import Certificate Summary** page, verify that the information is correct and then click **Next**.
9. On the **Executing Commands** page, verify that the **Task status** is **Completed** and then click **Finish**.
10. In the **Certificate Wizard**, select **External Edge certificate (public internet)** and then click **Assign**.
11. On the **Certificate Assignment** page, click **Next**.
12. On the **Certificate Store** page, click **View Certificate Details** to verify that you installed the correct certificate.
13. In the **Certificate** window, review the certificate information, and then click **OK**
14. On the **Certificate Store** page, click **Next**
15. On the **Executing Commands** page, verify that the **Task status** is **completed**, and then click **Finish**.
16. On the **Certificate Store** page, click **Next**.
17. To verify that your certificate was properly installed, in the Certificate Wizard, make sure that the status of the **External Edge certificate (public internet)** is **Assigned**.
18. Your SSL certificate has been successfully installed and assigned.

If you are unable to use these instructions for your server, we recommend that you contact either the vendor of your software or the organization that supports it.

ABOUT ACMETEK

“Acmetek is a Global Distributor and a Trusted Advisor of PKI /IoT & SSL Security Products and Managed Services Company.”

Acmetek Global Solutions, Inc. is a privately held Digital Security Services Company serving USA & APAC clients in website security solutions since 2010. The firm specializes in providing insight and expertise to enterprises, SMBs, governments, and provides a full range of Security Products, SSL, PKI, IoT, Malware Identity Scanning’s, Vulnerability Assessments, and Two-Factor Authentication.

Acmetek is a managed service partner of multi-brand technology solutions like CDW. We manage the Certificate Authority Practices of leading Website Security Brand, DigiCert (formerly known as Symantec). Over a decade of experience in the security industry empowered us to grow as an Authorized Distributor/ Platinum Partner for DigiCert and a leading provider of security solutions and services.

SSL Cert Free Trial | **MPKI** | **Request a Call Back** | **SSL Support Desk**

Our Web Security Solutions

SSL CERTIFICATES

Domain Validation

Activates HTTPS with a padlock. This SSL can issue in minutes.

Organization Validation

Activates HTTPS with a padlock. It validates an organization by providing a trust seal.

Extended Validation

Activates HTTPS with a padlock. It validates the organization by providing the company name before the domain name directly on the browser.

Code Signing Certificates

Protects users from downloading compromised software, prevents tampering, and provides the trusted assurance of authentication.

MPKI SOLUTIONS

Email Certificates

Using an Email certificate for user authentication encrypts transmission and signs the message,delivering comprehensive benefits for the sender and receiver.

Document Signing Certificates

Document signing certificates allow individuals, teams, and organizations to add an electronic, digital signature to a document in a variety of file formats to prove ownership.

Device Certificate

Verify identity, encrypt communications, and secures all home networks for internet connected devices before and after manufacturing.

MDM (Mobile Device Management)

Get a comprehensive look at mobile devices, master mobile email, and application rollout while protecting all data anddevices.

WIFI Certificates

Increases trust in public hotspots and protect user data.